

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10283320 A**

(43) Date of publication of application: **23 . 10 . 98**

(51) Int. Cl. **G06F 15/00**
G06F 9/06
G06F 19/00
G07F 7/08

(21) Application number: **10005411**

(22) Date of filing: **14 . 01 . 98**

(30) Priority: **05 . 02 . 97 JP 09 22256**

(71) Applicant: **NTT DATA:KK**

(72) Inventor: **NAKAJIMA YUSAKU**
MORI HIROYOSHI

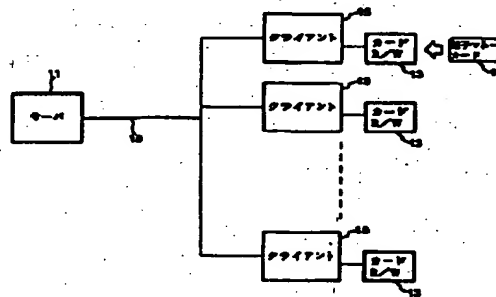
**(54) PRIVACY SYSTEM AND SECRET PROGRAM
MANAGEMENT SYSTEM AND RECORDING
MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To increase the level of security, and to attain realization by general hardware.

SOLUTION: A client 15 reads user information stored in an electronic money card 19 mounted on a card reader/writer, and transmits it to a server 11. The server 11 receives the user information from the client 15, and transmits an IC card writing program being a privacy program to the client 15. The client 15 executes the received IC card writing program, deletes the program after completing the execution, and transmits a deletion completion telegraphic message to the server 11. The server 11 waits for the deletion completion telegraphic message from the client 15 in a prescribed time after transmitting the IC card writing program to the client 15. When the server 11 does not receive the deletion completion telegraphic message in the prescribed time, the server 11 specifies an unauthorized user from the user information received from the client 15.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-283320

(43) 公開日 平成10年(1998)10月23日

(51) Int.Cl. ⁶	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 A
9/06	5 5 0	9/06 5 5 0 Z
19/00		15/30 C
G 0 7 F 7/08		3 5 0 A
		Z
		G 0 7 F 7/08 Z
		審査請求 未請求 請求項の数15 O L (全 14 頁)

(21) 出願番号 特願平10-5411

(22) 出願日 平成10年(1998) 1月14日

(31) 優先権主張番号 特願平9-22256

(32) 優先日 平9(1997) 2月5日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(72) 発明者 中島 雄作

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72) 発明者 森 啓悦

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

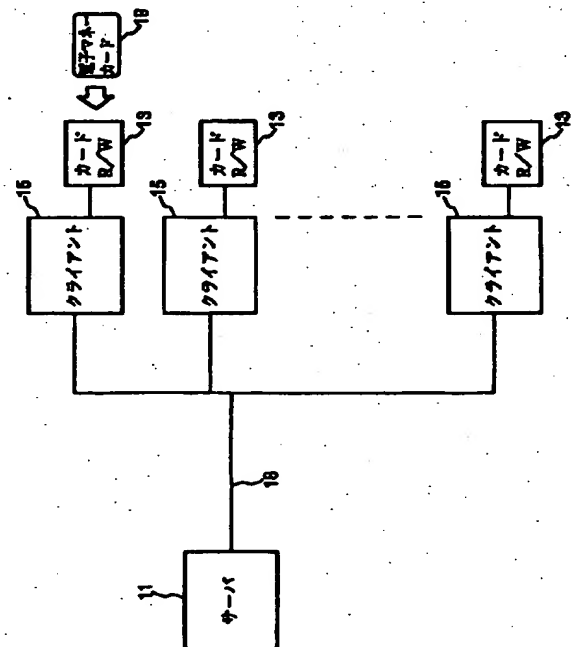
(74) 代理人 弁理士 木村 潤

(54) 【発明の名称】 セキュリティシステム、機密プログラム管理方法及び記録媒体

(57) 【要約】

【課題】 セキュリティのレベルが高く、汎用的なハードウェアで実現可能なセキュリティシステム、機密プログラム管理方法及び記録媒体を提供する。

【解決手段】 クライアント15は、カードR/W13に装着された電子マネーカード19に記憶されている利用者情報を読み出し、サーバ11に送信する。サーバ11は、クライアント15から利用者情報を受信すると、機密プログラムであるICカード書込プログラムをクライアント15に送信する。クライアント15は、受信したICカード書込プログラムを実行し、実行完了後、そのプログラムを削除すると共に、削除完了電文をサーバ11に送信する。サーバ11は、ICカード書込プログラムをクライアント15に送信した後、クライアント15からの削除完了電文を所定時間待つ。削除完了電文を所定時間内に受信しない場合、サーバ11は、クライアント15から受信した利用者情報より不正者を特定する。



【特許請求の範囲】

【請求項1】サーバと、該サーバに接続された複数のクライアントと、を備えるクライアントサーバシステムにおいて、

前記サーバは、

機密情報を含む機密プログラムを記憶する機密プログラム記憶手段と、

前記クライアントからの要求に応じて、前記機密プログラム記憶手段に記憶されている前記機密プログラムを要求元の前記クライアントに送信する手段と、を備え、

前記クライアントは、

前記機密プログラムを前記サーバに要求する要求送信手段と、前記機密プログラムを受信する受信手段と、前記受信手段により受信された前記機密プログラムを記憶する記憶手段と、前記記憶手段により記憶された前記機密プログラムを実行する実行手段と、前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段と、を備える、

ことを特徴とするセキュリティシステム。

【請求項2】前記クライアントは、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段と、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段と、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段と、を備え、

前記クライアントの前記削除手段は、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する手段を備える、

ことを特徴とする請求項1に記載のセキュリティシステム。

【請求項3】前記クライアントは、少なくとも前記ロック解除指示手段及び前記削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備える、

ことを特徴とする請求項2に記載のセキュリティシステム。

【請求項4】前記クライアントは、前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成して記憶するダミーファイル作成手段と、前記作成されたダミーファイルを削除するダミーファイル削除手段と、をさらに備える、

ことを特徴とする請求項2に記載のセキュリティシステム。

【請求項5】前記クライアントは、少なくとも前記ロック解除指示手段、前記削除手段、前記ダミーファイル作

成手段及び前記ダミーファイル削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備える、

ことを特徴とする請求項4に記載のセキュリティシステム。

【請求項6】前記クライアントの前記削除手段は、前記機密プログラムの削除後、削除の完了を示す削除完了電文を前記サーバに送信する手段を備え、

前記サーバは、前記機密プログラムの送信先の前記クライアントから前記削除完了電文を該機密プログラム送信時から所定時間内に受信したか否かを判別する判別手段と、前記削除完了電文を前記所定時間内に受信しなかったと判別された場合、不正検出を通知する手段と、を備える、

ことを特徴とする請求項1乃至5のいずれか1項に記載のセキュリティシステム。

【請求項7】前記クライアントは、該クライアントの利用者を特定する利用者情報を取得する取得手段を備え、前記クライアントの前記要求送信手段は、前記機密プログラムの要求を前記取得手段により取得された前記利用者情報と共に送信する手段を備え、

前記サーバは、前記判別手段により、前記削除完了電文を前記所定時間内に受信しなかったと判別された場合、前記クライアントから受信した前記利用者情報から不正者を特定し、通知する手段を備える、

ことを特徴とする請求項6に記載のセキュリティシステム。

【請求項8】機密プログラムを該機密プログラム保存用の第1の端末に格納するステップと、

前記機密プログラムを実行する第2の端末に前記第1の端末に記憶されている該機密プログラムを転送する転送ステップと、

前記転送ステップにより前記機密プログラムが転送された前記第2の端末において、該機密プログラムを実行し、実行終了後、該機密プログラムを削除する削除ステップと、

を備え、前記機密プログラムの保存と実行を別個の端末で実行することを特徴とする機密プログラム管理方法。

【請求項9】該機密プログラム管理方法は、

前記第2の端末に前記機密プログラムが記憶された際に、該機密プログラムへのアクセスに関する排他制御を行うロックステップと、

前記第2の端末における前記機密プログラムの実行終了後、該機密プログラムへの排他制御を解除するロック解除ステップと、を備え、

前記削除ステップは、前記ロック解除ステップにより前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記第2の端末から削除するステップを備える、

ことを特徴とする請求項8に記載の機密プログラム管理

方法。

【請求項10】該機密プログラム管理方法は、
前記第2の端末に前記機密プログラムが記憶された際に、該機密プログラムへのアクセスに関する排他制御を行うロックステップと、
前記第2の端末における前記機密プログラムの実行終了後、該機密プログラムへの排他制御を解除するロック解除ステップと、を備え、
前記削除ステップは、前記ロック解除ステップにより前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記第2の端末から削除するステップを備え、
該機密プログラム管理方法は、前記削除ステップによる前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成記憶するステップと、前記作成されたダミーファイルを削除するステップと、をさらに備える、
ことを特徴とする請求項8に記載の機密プログラム管理方法。

【請求項11】前記削除ステップにより前記機密プログラムが削除された後、削除の完了を前記第1の端末に通知する通知ステップと、
前記第1の端末が、前記通知ステップによる削除の完了の通知を、前記転送ステップによる前記機密プログラムの転送時から所定時間内に受信したか否かを判別する判別ステップと、
前記第1の端末が前記削除の完了の通知を前記所定時間内に受信していないと判別された場合、不正の検出を通知するステップと、
を更に備えることを特徴とする請求項8乃至10のいずれか1項に記載の機密プログラム管理方法。

【請求項12】前記転送ステップにより前記機密プログラムが転送された前記第2の端末において、該第2の端末の利用者を特定する利用者情報を取得する取得ステップと、
前記取得ステップより取得された前記利用者情報を前記第1の端末に送信するステップと、
前記判別ステップにより、前記第1の端末が前記削除の完了の通知を前記所定時間内に受信していないと判別された場合、前記利用者情報から不正者を特定し、通知するステップと、
を更に備えることを特徴とする請求項11に記載の機密プログラム管理方法。

【請求項13】コンピュータを、
機密情報を含む機密プログラムを要求する要求手段、
前記機密プログラムを受信する受信手段、
前記受信手段により受信された前記機密プログラムを記憶する記憶手段、
前記記憶手段により記憶された前記機密プログラムを実行する実行手段、

前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

- 【請求項14】コンピュータを、
機密情報を含む機密プログラムを要求する要求手段、
前記機密プログラムを受信する受信手段、
前記受信手段により受信された前記機密プログラムを記憶する記憶手段、
10 前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、
前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、
前記記憶手段により記憶された前記機密プログラムを実行する実行手段、
前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、
20 前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
- 【請求項15】コンピュータを、
機密情報を含む機密プログラムを要求する要求手段、
前記機密プログラムを受信する受信手段、
前記受信手段により受信された前記機密プログラムを記憶する記憶手段、
30 前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、
前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、
前記記憶手段により記憶された前記機密プログラムを実行する実行手段、
前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、
40 前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、
前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成記憶するダミーファイル作成手段、
前記作成されたダミーファイルを削除するダミーファイル削除手段、
50 として機能させるためのプログラムを記録したコンピュ

ータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機密性の高いプログラムを有するコンピュータシステムを、汎用的なハードウェアで実現可能なセキュリティシステム、機密プログラム管理方法及び記録媒体に関する。

【0002】

【従来の技術】高いレベルのセキュリティが必要とされるコンピュータシステムの一例として、金銭的価値を有する電子マネーをICカードに格納して使用する電子マネーシステムが考えられる。

【0003】このような電子マネーシステムでは、ICカードへの電子マネーの不正な書き込み等を防止するため、機密性の高い情報（例えば、ICカードへアクセスするためのパスワード）を含むプログラムは、第三者により容易に取得されないよう、強化されたハードウェアに記憶されることが望ましい。また、第三者がその機密性の高いプログラムにアクセスできないよう、利用者のオペレーションを制限することが望ましい。

【0004】また、そのようにして機密性の高い情報を強固なハードウェアに記憶しても、ハードウェアを破壊する等の行為により、その情報を記憶する記憶媒体が奪取される場合が考えられる。この場合、記憶媒体を奪取した者を特定するため、ハードウェアを常時監視することが望ましい。

【0005】

【発明が解決しようとする課題】上述したように、機密性の高いプログラムを有するコンピュータシステムでは、利用者のオペレーションが制限され、又、物理的に強固である特殊なハードウェアとそのハードウェアの監視とが必要とされていた。よって、パソコン等の汎用的なハードウェアを用いたシステムの構築は困難であった。また、ハードウェアの設置場所が常時監視可能な場所（例えば、監視カメラ又は係員による監視が可能な場所）に制限されていた。

【0006】本発明は、上記実状に鑑みてなされたもので、セキュリティのレベルが高く、汎用的なハードウェアで実現可能なセキュリティシステム、機密プログラム管理方法及び記録媒体を提供することを目的とする。また、任意の場所に設置可能なセキュリティシステム、機密プログラム管理方法及び記録媒体を提供することを他の目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点に係るセキュリティシステムは、サーバと、該サーバに接続された複数のクライアントと、を備えるクライアントサーバシステムにおいて、前記サーバは、機密情報を含む機密プログラムを記憶する機密プログラム記憶手段と、前記クライアントからの

要求に応じて、前記機密プログラム記憶手段に記憶されている前記機密プログラムを要求元の前記クライアントに送信する手段と、を備え、前記クライアントは、前記機密プログラムを前記サーバに要求する要求送信手段と、前記機密プログラムを受信する受信手段と、前記受信手段により受信された前記機密プログラムを記憶する記憶手段と、前記記憶手段により記憶された前記機密プログラムを実行する実行手段と、前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段と、を備える。

【0008】このような構成によれば、機密性の高いプログラムをサーバで一元管理し、クライアントで機密プログラムを実行する必要が生じた場合のみ、そのクライアントに機密プログラムを転送し、転送先で機密プログラムの実行が完了した後、その転送先における機密プログラムを削除する。これにより、機密プログラムは、使用時のみクライアントに存在し、通常はクライアントに存在しない。よって、クライアントでは機密プログラムを常時格納するための特殊なハードウェアが不要となるため、クライアントを汎用的なハードウェアで構成することができる。

【0009】前記クライアントは、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段と、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段と、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段と、を備えてもよく、前記クライアントの前記削除手段は、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する手段を備えてもよい。これにより、機密性の高い情報を含む機密プログラムがクライアントの記憶手段に記憶されている間、その機密プログラムに対してロックをかけることにより、第三者等によりいかなるオペレーションが行われようとも、機密プログラムへのアクセスを防ぐことができる。

【0010】前記クライアントは、少なくとも前記ロック解除指示手段及び前記削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備えてもよい。

【0011】前記クライアントは、前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成して記憶するダミーファイル作成手段と、前記作成されたダミーファイルを削除するダミーファイル削除手段と、をさらに備えてもよい。これにより、機密性の高い情報を含む機密プログラムに対してロックをかけて第三者がアクセスできない状態でダミーファイルで上書きし、完全

に削除して復元不可能とすることにより、セキュリティをより高めることができる。

【0012】前記クライアントは、少なくとも前記ロック解除指示手段、前記削除手段、前記ダミーファイル作成手段及び前記ダミーファイル削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備えてもよい。

【0013】前記クライアントの前記削除手段は、前記機密プログラムの削除後、削除の完了を示す削除完了電文を前記サーバに送信する手段を備えてもよく、前記サーバは、前記機密プログラムの送信先の前記クライアントから前記削除完了電文を該機密プログラム送信時から所定時間内に受信したか否かを判別する判別手段と、前記削除完了電文を前記所定時間内に受信していないと判別された場合、不正検出を通知する手段と、を備えてもよい。

【0014】このような構成によれば、機密プログラム送信時から所定時間内に、機密プログラムの転送先のクライアントから削除完了電文を受信したか否かを判別することにより、機密プログラムが奪取されたことを検出できる。

【0015】前記クライアントは、該クライアントの利用者を特定する利用者情報を取得する取得手段を備えてもよく、前記クライアントの前記要求送信手段は、前記機密プログラムの要求を前記取得手段により取得された前記利用者情報と共に送信する手段を備えてもよく、前記サーバは、前記判別手段により、前記削除完了電文を前記所定時間内に受信しなかったと判別された場合、前記クライアントから受信した前記利用者情報から不正者を特定し、通知する手段を備えてもよい。

【0016】このような構成によれば、機密プログラムが奪取された場合、利用者情報から不正者を特定することができる。よって、不正者を監視するためにクライアントの設置場所を限定することが不要となり、任意の場所にクライアントを設置することができる。

【0017】また、この発明の第2の観点に係る機密プログラム管理方法は、機密プログラムを該機密プログラム保存用の第1の端末に格納するステップと、前記機密プログラムを実行する第2の端末に、前記第1の端末に記憶されている該機密プログラムを転送する転送ステップと、前記転送ステップにより前記機密プログラムが転送された前記第2の端末において、該機密プログラムを実行し、実行完了後、該機密プログラムを削除する削除ステップと、を備える。

【0018】このような構成によれば、機密性の高いプログラムを第1の端末で一元管理し、第2の端末で機密プログラムを実行する場合のみ、その第2の端末に機密プログラムを転送し、転送先で機密プログラムの実行が完了した後、その転送先における機密プログラムを削除する。これにより、機密プログラムは、使用時のみ第2

の端末に存在し、通常は存在しない。よって、第2の端末では機密プログラムを常時格納するための特殊なハードウェアを設ける必要がなくなり、第2の端末を汎用的なハードウェアで構成することができる。

【0019】前記削除ステップにより前記機密プログラムが削除された後、削除の完了を前記第1の端末に通知する通知ステップと、前記第1の端末が、前記通知ステップによる削除の完了の通知を、前記転送ステップによる前記機密プログラムの転送時から所定時間内に受信したか否かを判別する判別ステップと、前記第1の端末が前記削除の完了の通知を前記所定時間内に受信していないと判別された場合、不正の検出を通知するステップと、を更に備えてもよい。

【0020】このような構成によれば、機密プログラムの削除の完了の通知を転送先の第2の端末から機密プログラム送信時より所定時間内に受信したか否かを判別することにより、機密プログラムが不正に奪取されたことを検出することができる。

【0021】該機密プログラム管理方法は、前記第2の端末に前記機密プログラムが記憶された際に、該機密プログラムへのアクセスに関する排他制御を行うロックステップと、前記第2の端末における前記機密プログラムの実行終了後、該機密プログラムへの排他制御を解除するロック解除ステップと、を備えてもよく、前記削除ステップは、前記ロック解除ステップにより前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記第2の端末から削除するステップを備えてもよい。

【0022】また、該機密プログラム管理方法は、前記削除ステップによる前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成記憶するステップと、前記作成されたダミーファイルを削除するステップと、をさらに備えてもよい。

【0023】前記転送ステップにより前記機密プログラムが転送された前記第2の端末において、該第2の端末の利用者を特定する利用者情報を取得する取得ステップと、前記取得ステップより取得された前記利用者情報を前記第1の端末に送信するステップと、前記判別ステップにより、前記第1の端末が前記機密プログラムの削除の完了の通知を前記所定時間内に受信していないと判別された場合、前記利用者情報から不正者を特定し、通知するステップと、を更に備えてもよい。

【0024】このような構成によれば、機密プログラムが奪取された場合、利用者情報から不正者を特定することができる。よって、不正者を監視するために第2の端末の設置場所を限定することが不要となり、任意の場所に第2の端末を設置することができる。

【0025】また、この発明の第3の観点に係る記録媒体は、コンピュータを、機密情報を含む機密プログラム

を要求する要求手段、前記機密プログラムを受信する受信手段、前記受信手段により受信された前記機密プログラムを記憶する記憶手段、前記記憶手段により記憶された前記機密プログラムを実行する実行手段、前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段、として機能させるためのプログラムを記録する。

【0026】また、この発明の第4の観点に係る記録媒体は、コンピュータを、機密情報を含む機密プログラムを要求する要求手段、前記機密プログラムを受信する受信手段、前記受信手段により受信された前記機密プログラムを記憶する記憶手段、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、前記記憶手段により記憶された前記機密プログラムを実行する実行手段、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、として機能させるためのプログラムを記録する。

【0027】また、この発明の第5の観点に係る記録媒体は、コンピュータを、機密情報を含む機密プログラムを要求する要求手段、前記機密プログラムを受信する受信手段、前記受信手段により受信された前記機密プログラムを記憶する記憶手段、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、前記記憶手段により記憶された前記機密プログラムを実行する実行手段、前記実行手段による前記機密プログラムへの排他制御の解除を指示するロック解除指示手段、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成して記憶するダミーファイル作成手段、前記作成されたダミーファイルを削除するダミーファイル削除手段、として機能させるためのプログラムを記録する。

【0028】

【発明の実施の形態】本発明の実施の形態にかかるセキュリティシステムについて、金銭的価値を有する電子マネーを格納するICカード（電子マネーカード）を使用する電子マネーシステムを例に、以下図面を参照して説

明する。この電子マネーシステムは、図1に示すように、サーバ11と、カードリーダー/ライター（以下、カードR/W）13を備えるクライアント15と、これらを接続するネットワーク18と、電子マネーカード19と、より構成される。

【0029】サーバ11の論理構成図（ソフトウェア構成図）を図2に示す。図示されるように、サーバ11は、通信制御プログラム21と、ファイル伝送プログラム23と、ICカード読み込みプログラム25と、サーバプログラム27と、OS（Operating System）29と、を備える。

【0030】通信制御プログラム21は、外部と通信を行うための制御プログラムであり、例えばTCP/IPプロトコル、LANドライバ等から構成される。ファイル伝送プログラム23は、ファイルを伝送するためのプログラムであり、例えばFTP（File Transfer Protocol）等から構成される。ICカード読み込みプログラム25は、電子マネーカード19への読み込みを行うためのプログラムであり、読み込みを行う際に必要なパスワードを含む。サーバプログラム27は、後述するクライアント15のクライアントプログラムと通信するためのプログラムである。OS29は、サーバ11全体を管理するためのプログラムである。

【0031】この電子マネーシステムにおける機密性の高い情報とは、例えば電子マネーカード19にデータを書き込むために必要なパスワードである。よって、この情報を有するICカード読み込みプログラム25が本システムにおける機密性の高いプログラムである。

【0032】クライアント15の論理構成図を図3に示す。図示されるように、クライアント15は、通信制御プログラム31と、ファイル伝送プログラム33と、クライアントプログラム35と、ICカードR/Wドライバ37と、OS39と、を備える。

【0033】通信制御プログラム31とファイル伝送プログラム33とOS39とは、上述したサーバ11の通信制御プログラム21とファイル伝送プログラム23とOS29とそれぞれ同等の機能を有するプログラムである。クライアントプログラム35は、サーバプログラム27との通信、サーバ11からのファイル伝送、クライアント15に格納されているプログラムの起動、ICカードR/Wドライバ37を介した電子マネーカード19とのデータの送受信、等を行うためのプログラムである。ICカードR/Wドライバ37は、カードR/W13を制御するためのプログラムである。なお、本システムでは、電子マネーカード19に書き込みをするためにはパスワードが必要であり、ICカードR/Wドライバ37は、このパスワードのチェック等も行う。

【0034】サーバ11のシステム構成図を図4に示す。図示されるように、サーバ11は、CPU41と、メモリ42と、入力装置43と、表示装置44と、補助

記憶装置45と、通信制御装置46と、を備える。図2を参照して上述したサーバ11側のプログラムは、メモリ42又は補助記憶装置45に格納されており、例えばメモリ42に常駐していないプログラムは、実行時に補助記憶装置45からメモリ42にロードされ、CPU41により実行される。通信制御部46は、CPU41からの指示により、クライアント15との通信を行う。

【0035】クライアント15のシステム構成図を図5に示す。図示されるように、クライアント15は、CPU51と、メモリ52と、入力装置53と、表示装置54と、補助記憶装置55と、通信制御装置56と、ICカードR/W制御装置57と、を備える端末である。クライアント15は、カードR/W13とクライアント15を接続し、カードR/W13を制御するためのICカードR/W制御装置57を備える点以外は、上述したサーバ11と同様の構成を有する。

【0036】電子マネーカード19は、図6に示すように、その電子マネーカード19の所有者の情報である利用者情報と、その電子マネーカード19の利用履歴と、残高を記憶する。利用者情報は、利用者ID、氏名、住所、電話番号等を含む。

【0037】この電子マネーシステムは、電子マネーカード19にデータを書き込むためのパスワードを含むICカード番込プログラム25を、サーバ11のみに格納する。そして、クライアント15でそのプログラムを実行する必要が生じた際に、サーバ11から転送し、実行終了後、プログラムをクライアント15から削除することにより、高レベルのセキュリティを保持する。ICカード番込プログラム25をサーバ11からクライアント15に転送し、転送したプログラムの実行完了後、そのプログラムを消去する機密プログラム転送処理について図7、図8を参照して説明する。

【0038】まず、クライアント15での処理を図7のフローチャートを用いて説明する。利用者により電子マネーの取引の指示がクライアント15に入力され、この入力に回答し、クライアントプログラム35が利用者の電子マネーカード19に記憶されている利用者を特定する情報（利用者情報）をICカードR/Wドライバ37を介して読み出す（ステップS1）。次に、クライアントプログラム35は、読み出した利用者情報を、通信制御プログラム31を介してサーバ11に送信する（ステップS2）。

【0039】送信した利用者情報に回答してサーバ11から送信されたICカード番込プログラム25を、ファイル転送プログラム33が通信制御プログラム31を介して受信し、クライアントプログラム35に渡す（ステップS3）。クライアントプログラム35は、受信したICカード番込プログラム25を実行する（ステップS4）。実行終了後、クライアントプログラム35は、ICカード番込プログラム25を削除し（ステップS

5）、機密プログラムの削除の完了を示す削除完了電文を通信制御プログラム31を介してサーバ11に送信する（ステップS6）。

【0040】次に、サーバ11での処理を図8のフローチャートを用いて説明する。サーバ11の通信制御プログラム21は、クライアント15からの利用者情報を受信し、サーバプログラム27に渡す（ステップS11）。サーバプログラム27は、利用者情報を受信すると、ICカード番込プログラム25をクライアント15へ送信するようファイル転送プログラム23に指示する。この指示に回答して、ファイル転送プログラム23は、ICカード番込プログラム25を通信制御プログラム21を介してクライアント15に転送する（ステップS12）。

【0041】サーバプログラム27は、ICカード番込プログラム25をクライアント15に転送した後、そのクライアント15からの削除完了電文を所定時間待つ（ステップS13）。所定時間内にクライアント15から削除完了電文を受信した場合、処理を終了する。所定時間が経過しても、クライアント15から削除完了電文が到着しない場合、機密プログラムが奪取された等、不正検出の旨のエラーメッセージを表示する。また、サーバプログラム27は、今回の処理においてクライアント15から受信した利用者情報から不正者を特定し、管理者等に通知する（ステップS14）。

【0042】上述のように、機密性の高いICカード番込プログラム25をサーバ11からクライアント15に転送し、使用後に削除することにより、ICカード番込プログラム25をクライアント15に常駐させなくてもよい。このため、クライアント15のハードウェアを強化したり、利用者のオペレーションを限定する必要がなくなる。また、機密性の高いプログラムがクライアント15に格納されている間に、そのプログラムが記憶されているハードウェアが利用者により奪取された場合は、削除完了電文がサーバ11に返らないことから、その不正を検知することができる。また、不正を検出した場合、サーバ11は、クライアント15から受信した利用者情報により、不正者を特定することができる。

【0043】次に、この電子マネーシステムで、利用者Aが自己の電子マネーカード19を用いて、クライアント15Bで買い物をする場合について、図9を参照して説明する。なお、この電子マネーシステムでは、利用者がクライアント15Bの表示装置54に表示された物品の中から、購入したい物品を入力装置53より入力し、入力された物品が、後日、利用者に発送されることとする。

【0044】利用者Aは、自己の電子マネーカード19をクライアント15Bに接続されているカードR/W13に装着し、表示装置54に表示されている物品の中から所望の物品を選択し、入力装置53から購入要求を入

力する。クライアント15Bのクライアントプログラム35は、この購入要求に応答し、ICカードR/Wドライバ37を介して、カードR/W13に装着されている電子マネーカード19から利用者Aの利用者情報を読み出す(図9(A)P1)。次に、クライアントプログラム35は、読み出した利用者情報を、通信制御プログラム31を介してサーバ11に送信する(P2)。

【0045】サーバ11の通信制御プログラム21は、クライアント15Bから利用者情報を受信し、サーバプログラム27に送る。サーバプログラム27は、通信制

御プログラム21からの利用者情報に応答して、クライアント15BへICカード申込プログラム25を転送するようファイル転送プログラム23に指示する(図9(B)P3)。ファイル転送プログラム23は、この指示に応答し、ICカード申込プログラム25を通信制御プログラム21を介してクライアント15Bに転送する(P4)。サーバプログラム27は、ICカード申込プログラム25の送信後、所定時間(例えば、5分間)、クライアント15Bからの削除完了電文を待つ。

【0046】クライアント15Bのファイル転送プログラム33は、通信制御プログラム31を介してICカード申込プログラム25を受信し、クライアントプログラム35に渡す。クライアントプログラム35は、ICカード申込プログラム25を起動する。起動されたICカード申込プログラム25は、自己が有するパスワードを用いて、ICカードR/Wドライバ37を介してICカードにアクセスする。ICカード申込プログラム25は、電子マネーカード19の利用履歴として利用者Aが購入した物品の情報(例えば、物品を特定するためのコード、価格、購入日等)を書き込み、その電子マネーカードに記憶されている電子マネーの残高から物品の価格を差し引く(図9(C)P5)。

【0047】ICカード申込プログラム25の処理(電子マネーカード19への書き込み)が終了すると、クライアントプログラム35は、ICカード申込プログラム25を削除し(図9(D)P6)、プログラムの削除の完了を示す削除完了電文を通信制御プログラム31を介してサーバ11に送信する(P7)。また、クライアントプログラム35は、ICカードR/Wドライバ37を介して、カードR/W13に装着された電子マネーカード19を排出する。サーバプログラム27は、クライアント15Bから削除完了電文を受信し、処理を終了する。

【0048】また、ICカード申込プログラム25がクライアント15Bに存在している間に、利用者Aがクライアント15B全体又はICカード申込プログラム25が記憶されている補助記憶装置55を奪取する等の不正を行った場合(図9(E)P8)、クライアント15Bは削除完了電文をサーバ11に送信しない。この場合、サーバ11のサーバプログラム27は削除完了電文を受

信しないため、所定時間経過後、不正検出のメッセージを表示装置44に表示すると共に、クライアント15Bから受信した利用者情報より不正者が利用者Aであると特定し、その旨を表示する(P9)。

【0049】このようにして、ICカード申込プログラム25をサーバ11からクライアント15Bに転送し、使用後に削除することにより、クライアント15B上でICカード申込プログラム25を安全に動作させることができる。また、ICカード申込プログラム25がクライアント15Bに格納されている間に奪取された場合には、クライアント15Bから受信した利用者情報により、不正者を特定することができる。

【0050】なお、クライアント15が、サーバ11から上記ICカード申込プログラム25等の機密プログラムをファイル転送により受け取り、自己の記憶領域に記憶した際に、その機密プログラムに対してファイルロックをかけ、クライアントプログラム35以外からアクセスできないようにして、セキュリティを強化してもよい。この場合のクライアント15Cは、図10に示すように、上記クライアントプログラム35にファイルロック機能を追加したクライアントプログラム35Cを有する点以外は、上記クライアント15とほぼ同様の構成を有する。以下、このクライアント15Cの動作について図11のフローチャートを参照して説明する。

【0051】クライアント15Cは、例えば利用者による指示に応答し、利用者の電子マネーカード19の利用者情報をICカードR/Wドライバ37を介して読み出し、該利用者情報を通信制御プログラム31を介してサーバ11に送信する(ステップS11)。送信した利用者情報に応答してサーバ11から送信されたICカード申込プログラム25をファイル転送プログラム33が通信制御プログラム31を介して受信し、クライアントプログラム35Cに渡す(ステップS12)。これにより、ICカード申込プログラム25のファイルがクライアント15Cのハードディスクに作成される。

【0052】次に、クライアントプログラム35Cが、ICカード申込プログラム25のファイルに対しファイルロックをかけるよう指示するファイルロックコマンドをOS39に発行して、ICカード申込プログラム25のファイルをファイルロックする(ステップS13)。これにより、ICカード申込プログラム25は、クライアントプログラム35C以外からアクセスできなくなる。この状態でクライアントプログラム35CはICカード申込プログラム25を実行する(ステップS14)。実行終了後、クライアントプログラム35Cは、クライアント15C上で他のタスクが実行されないようにOS39にタスク切替禁止コマンドを発行し、タスクの切り替えを禁止する(ステップS15)。

【0053】コマンド発行後、クライアントプログラム35Cは、ICカード申込プログラム25のファイルロ

ックを解除するためのファイルロック解除コマンドをOS 39に発行し、ICカード申込プログラム25に対するファイルロックを解除する(ステップS16)。次に、クライアントプログラム35Cは、ICカード申込プログラム25を削除するための削除コマンドをOS 39に発行し、ICカード申込プログラム25を削除する(ステップS17)。削除コマンド発行後、クライアントプログラム35Cは、ステップS15で発行したタスク切替禁止コマンドを解除するための解除コマンドをOS 39に発行して、タスクの切り替えの禁止を解除し(ステップS18)、機密プログラムの削除の完了を示す削除完了電文を通信制御プログラム31を介してサーバ11に送信し(ステップS19)、処理を終了する。

【0054】このようにして、ICカード申込プログラム25等の機密性の高い情報を含むプログラムがクライアント15Cに格納されている間は、その機密プログラムに対してロックをかけることにより、第三者(利用者を含む)によりいかなるオペレーションが行われようとも、機密プログラムへのアクセスを防ぐことができる。なお、この場合のサーバ11の構成及び動作は上記と同様である。

【0055】また、上記クライアント15Cにおいて機密プログラムを削除した場合、FAT (File Access Table) 上では、機密プログラムは削除されているが、記憶ディスクにはその機密プログラムが残存している。この記憶ディスクに残存している機密プログラムに任意情報を上書きして完全に削除することにより、さらにセキュリティを強化してもよい。この場合のクライアント15Dは、図12に示すように、上記クライアントプログラム35Cに、上書きによる削除機能を追加したクライアントプログラム35Dを有する点以外は、上記クライアント15Cとほぼ同様の構成を有する。以下、このクライアント15Dの動作について図13のフローチャートを参照して説明する。

【0056】クライアント15Dは、例えば利用者による指示に応答し、利用者の電子マネーカード19の利用者情報をICカードR/Wドライバ37を介して読み出し、該利用者情報を通信制御プログラム31を介してサーバ11に送信する(ステップS21)。送信した利用者情報に応答してサーバ11から送信されたICカード申込プログラム25をファイル転送プログラム33が通信制御プログラム31を介して受信し、クライアントプログラム35Dに渡す(ステップS22)。これにより、ICカード申込プログラム25のファイルがクライアント15Dのハードディスクに作成される。

【0057】次に、クライアントプログラム35Dが、ICカード申込プログラム25に対するファイルロックコマンドを発行し(ステップS23)、ICカード申込プログラム25を実行する(ステップS24)。実行終了後、クライアントプログラム35Dは、タスク切替禁

止コマンドを発行して、タスクの切り替えを禁止する(ステップS25)。これにより、例えば第三者がICカード申込プログラム25に別のプログラムからアクセスしようとしてもできなくなる。

【0058】コマンド発行後、クライアントプログラム35Dは、ICカード申込プログラム25のファイルに対するファイルロック解除コマンドを発行し(ステップS26)、ICカード申込プログラム25を削除するための削除コマンドを発行する(ステップS27)。この時点では、FAT上ではICカード申込プログラム25のファイルが削除されたこととなるが、ICカード申込プログラム25のファイル自体は記憶ディスクから未だ削除されていない。

【0059】削除コマンド発行後、クライアントプログラム35Dは、ICカード申込プログラム25のファイルと同一のファイル名のダミーファイルを作成し記憶する(ステップS28)。これにより、記憶ディスクにおけるICカード申込プログラム25は、新規に作成された同一ファイル名のダミーファイルにより上書きされるため、ICカード申込プログラム25はハードディスクから完全に削除される。なお、ダミーファイルの内容は任意であり、例えば空白文字からなる1000バイトのファイルとしてもよい。ダミーファイル作成後、クライアントプログラム35Dは、そのダミーファイルを削除する削除コマンドを発行する(ステップS29)。ステップS29における削除コマンド実行後においても、ハードディスクにはダミーファイルが残存しているが、仮にそのダミーファイルを第三者に見られたとしても問題ない。

【0060】次に、クライアントプログラム35Dは、タスクの切り替えの禁止を解除するための解除コマンドを発行して(ステップS30)、処理を終了する。なお、必要に応じて、ステップS29の後で、機密プログラムの削除の完了を示す削除完了電文を通信制御プログラム31を介してサーバ11に送信してもよい。

【0061】このようにして、ICカード申込プログラム25等の機密性の高い情報を含むプログラムをクライアント15Dに転送した際、その機密プログラムに対してロックをかけて第三者がアクセスできない状態で、ハードディスク上でダミーファイルで上書きして完全に削除して復元不可能とすることにより、セキュリティをより高めることができる。なお、この場合のサーバ11の構成及び動作は上記と同様である。

【0062】なお、この発明は、電子マネーシステムに限定されず、機密性の高い情報を有するプログラムを実行する任意のコンピュータシステムに適用可能である。例えば、特定の社員だけが機密の回覧を見ることが出来る回覧システムとして実現してもよい。このシステムでは、例えば、回覧データにアクセスするためにはパスワードが必要であり、そのパスワードを含み、回覧データ

を表示する回覧表示プログラムがサーバに格納されている。社員がクライアントに入力した社員IDがサーバに送信され、サーバが、登録された社員IDか否かを判別し、登録されている場合、回覧表示プログラムをクライアントに転送し、実行後、削除するようにしてもよい。

【0063】サーバが乱数を生成し、機密プログラムと併せてクライアントに転送し、クライアントが、サーバから受信した乱数を削除完了電文に含めて送信するようにしてもよい。これにより、削除完了電文の偽造が困難となるため、機密プログラムを奪取した不正者が削除完了電文を偽造してサーバに送信することを防止することができる。また、サーバが暗号鍵を機密プログラムと共にクライアントに送信し、クライアントが、受信した暗号鍵で削除完了電文を暗号化して送信するようにしてもよい。

【0064】サーバ、クライアント間の通信を、RSA方式等を用いて暗号化してもよい。

【0065】なお、機密プログラムを機密プログラム保存用の端末に格納しておき、要求に応じて、その機密プログラム保存用の端末から要求元のクライアント(端末)に機密プログラムを転送するようにしてもよい。

【0066】また、上記説明におけるサーバ11及びクライアント15の論理構成は一例であり、これに限定されない。

【0067】なお、上述説明における通信制御プログラム21、ファイル転送プログラム23、ICカード書込プログラム25、サーバプログラム27を格納した媒体(フロッピーディスク、CD-ROM等)から該プログラムをインストールすることにより、上記サーバ11を実現してもよい。また、通信制御プログラム31、ファイル転送プログラム33、クライアントプログラム35を格納した媒体から該プログラムをインストールすることにより、上記クライアント15を実現してもよい。また、コンピュータに上記プログラムを供給するための媒体は、通信媒体(通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体)でも良い。例えば、通信ネットワークの掲示板(BBS)に該プログラムを掲示し、これをネットワークを介して配信してもよい。

【0068】

【発明の効果】以上説明したように、本発明によれば、機密性の高いプログラムをサーバで一元管理し、クライアントで実行する必要が生じた場合のみ、機密プログラムを転送し、機密プログラムの実行が完了した後、クライアントにおける機密プログラムを削除する。これにより、機密プログラムは、使用時のみクライアントに存在*

*し、通常はクライアントに存在しない。よって、クライアントでは機密プログラムを常時格納するための特殊なハードウェアを設ける必要がなく、クライアントを汎用的なハードウェアで構成することができる。また、機密プログラムが奪取された場合、利用者情報から不正者を特定することができるため、不正者を監視するためにクライアントの設置場所を限定することが不要となり、任意の場所にクライアントを設置することができる。

【図面の簡単な説明】

10 【図1】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図2】サーバの論理的構成を示す図である。

【図3】クライアントの論理的構成を示す図である。

【図4】サーバのシステム構成を示す図である。

【図5】クライアントのシステム構成を示す図である。

【図6】電子マネーカードに記憶されるデータの構造を示す図である。

【図7】クライアントにおける機密プログラム転送処理を説明するためのフローチャートである。

20 【図8】サーバにおける機密プログラム転送処理を説明するためのフローチャートである。

【図9】この電子マネーシステムにおける機密プログラム転送処理を具体的に説明するための図である。

【図10】ファイルロック機能を有する場合のクライアントの論理的構成を示す図である。

【図11】図10に示すクライアントにおける機密プログラム転送処理を説明するためのフローチャートである。

30 【図12】上書きによるファイル削除機能を有する場合のクライアントの論理的構成を示す図である。

【図13】図12に示すクライアントにおける機密プログラム転送処理を説明するためのフローチャートである。

【符号の説明】

11 サーバ

13 カードR/W

15、15C、15D クライアント

18 ネットワーク

19 電子マネーカード

40 21、31 通信制御プログラム

23、33 ファイル転送プログラム

25 ICカード書込プログラム

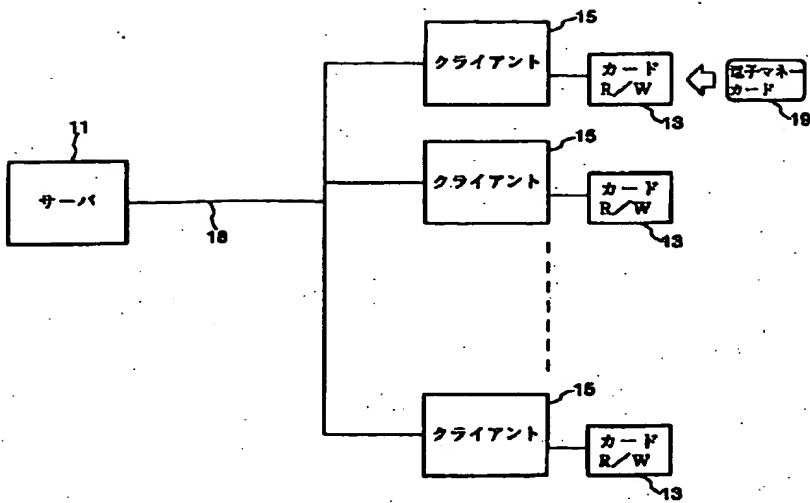
27 サーバプログラム

29、39 OS

35、35C、35D クライアントプログラム

37 ICカードR/Wドライバ

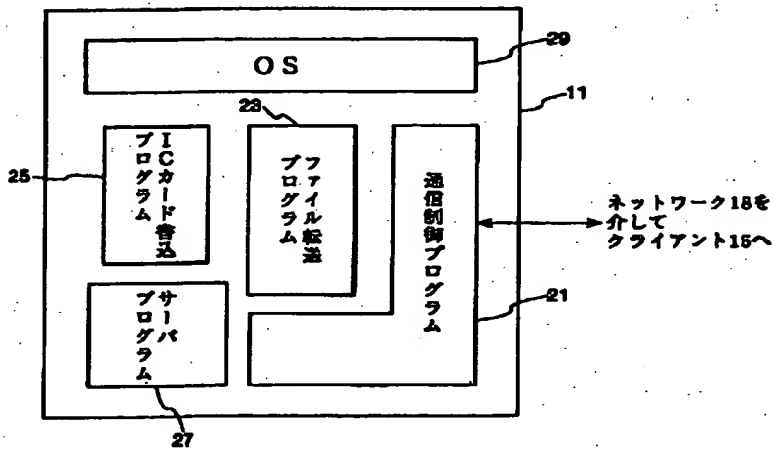
【図1】



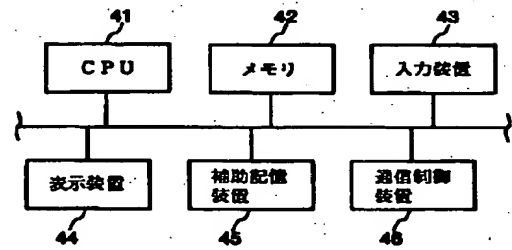
【図6】

利用者情報	利用者ID
	氏名
	住所
	電話番号
利用履歴	利用履歴A
	利用履歴B
	...
	残高

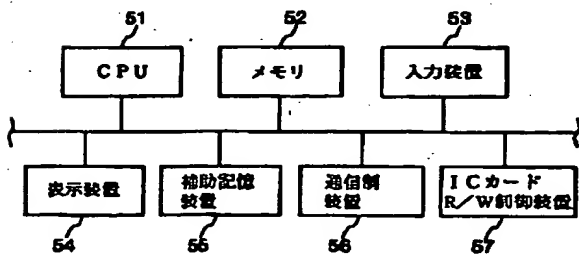
【図2】



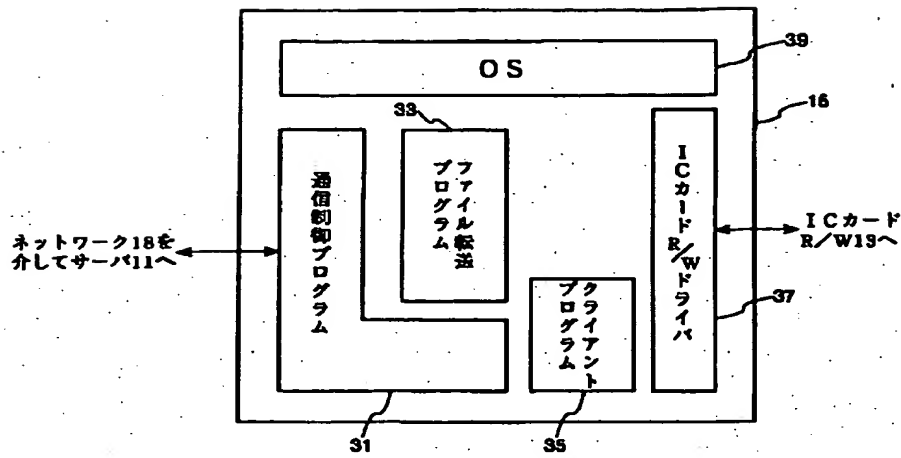
【図4】



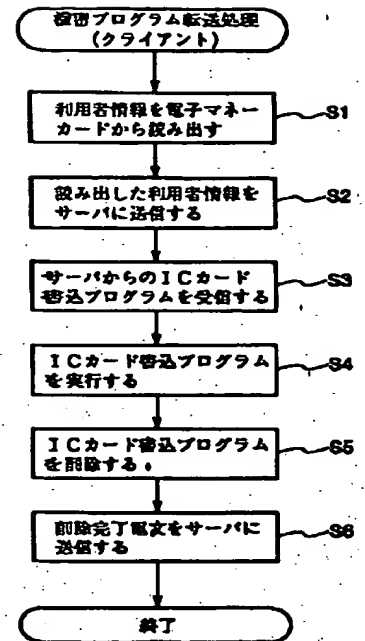
【図5】



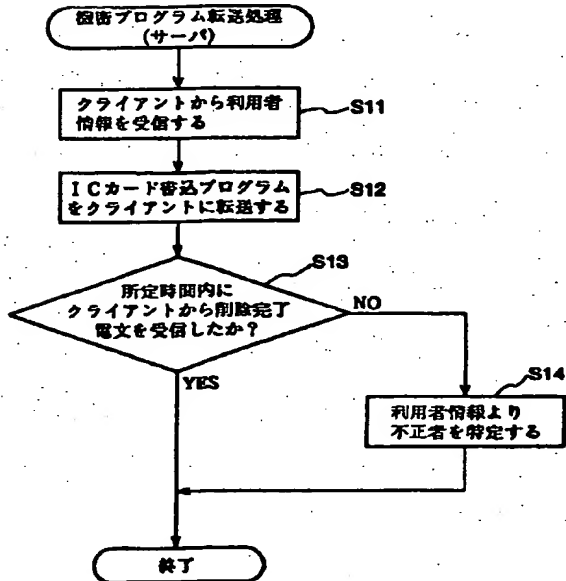
【図3】



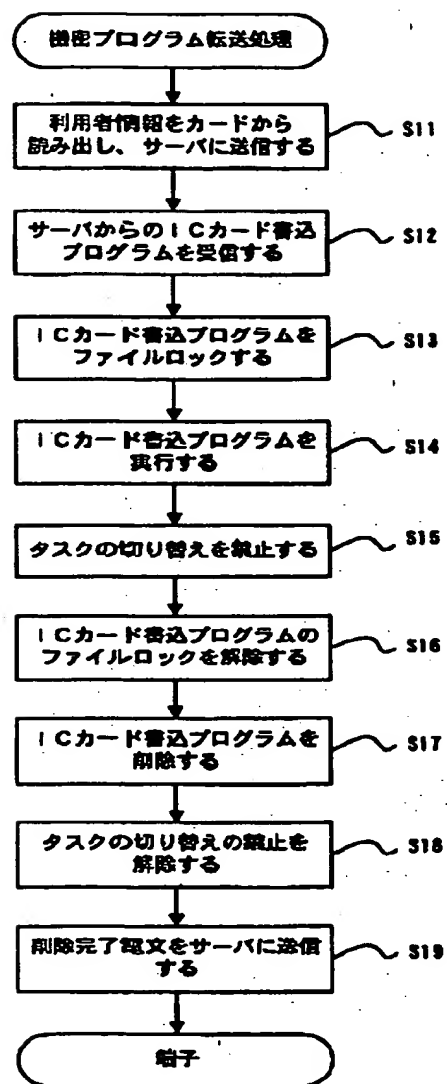
【図7】



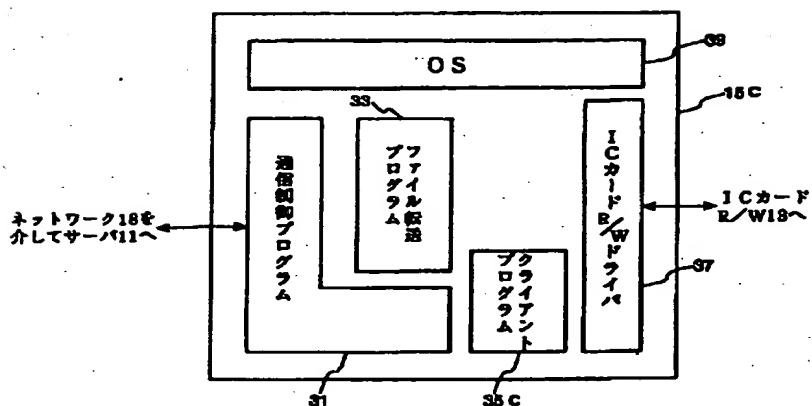
【図8】



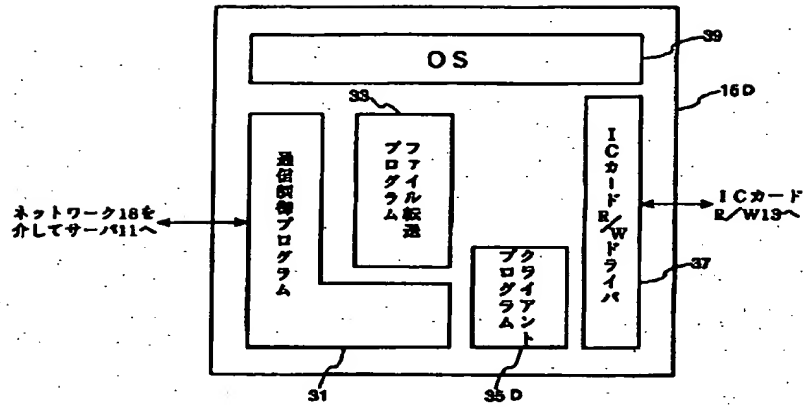
【圖 11】



【圖 10】



【図12】



【図13】

